UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/759,443	01/13/2001	Francisco Corella	10001558-2	9963

22879 7590 03/24/2005

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/759,443	CORELLA, FRANCISCO	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 December 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-59* is/are pending in the application.

4a) Of the above claim(s) *15 and 35* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14,16-34 and 36-59* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11/8/04, 2/17/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment filed on 06 December 2004 has been noted and made of record.

2. Claims 1-59 have been presented for examination.

3. Claims 15 and 35 have been cancelled without prejudice as per Applicant's request.

Response to Arguments

4. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. The Applicant merely alleges that the undesignated issue certificates are not equivalent to the unsigned public key validation certificate issued offline, the account information is not equivalent to the public key serial number, and that the free certificates are not equivalent to the disposable public key validation certificate. The Applicant at no time cites differences between the prior art language and the claim language.

5. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies, such as validating the subject's public key before using the public/private key pair for authentication purposes, in such a way that the public key will cease to be usable for authentication purposes if the subject notifies the PKVS that the private key has been compromised are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). As per claims 37-59, there is no mention made whatsoever of a

public key validation service, let alone that performs the functions disclosed in the Applicant's arguments made on page 15.

6. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies, such as one or more public key validation agents, each public key validation agent having a private/public key pair for a digital signature cryptosystem are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

7. See further rejections that follow.

Information Disclosure Statement

8. The information disclosure statement (IDS) submitted on 08 November 2004 was filed after the mailing date of the first office action on 02 September 2004. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

9. The information disclosure statement (IDS) submitted on 17 February 2005 was filed after the mailing date of the first office action on 02 September 2004. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Claim Rejections

10. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

11. Claims 1-8, 10, 14,15, 17-28, 30, 35 are rejected under 35 U.S.C. 102(b) as being anticipated by Ramasubramani (USP 6,233,577).

12. As per claims 1, 21 Ramasubramani teaches an off-line (landnet, col. 7, line 56) registration authority for issuing unsigned (undesignated) public key validation certificate (col. 7, lines 35-37) that binds a public key of the subject to a first public key serial number (ID) (col. 7, line 48), maintaining a certificate database (col. 7, line 38) which stores the unsigned PKVC, an online credentials server for issuing a disposable public key validation certificate to the subject (col. 7, lines 42-45) from the first unsigned PKVC, and maintain a table that contains entries corresponding to valid PKVCS (col. 7, lines 38-39).

13. As per claims 2, 22 Ramasubramani teaches the PKVN are unique (col. 7, line 1).

14. As per claims 3, 23 Ramasubramani teaches the subject can invalidate the first unsigned PKVC entry in the table (col. 12, lines 13-15).

15. As per claims 4, 24 Ramasubramani teaches the registration authority generates a public key revocation code to be used by the subject in its revocation request (col. 12, lines 1-11).

16. As per claims 5, 25 Ramasubramani teaches a secure channel that provides data (col. 7, lines 55-56).

17. As per claims 6, 26 Ramasubramani teaches an expiration date/time (col. 2, line 10).

18. As per claims 7, 27 Ramasubramani teaches a validity period from when the credentials server issues the disposable PKVC to the expiration date/time is sufficiently short such that the disposable PKVC does not need to be subject to revocation (col. 2, lines 10).

19. As per claims 8, 28 Ramasubramani teaches the disposable PKVC is not subject to revocation (col. 12, lines 5-7).

20. As per claims 10, 30 Ramasubramani teaches a PKVC is issued in response to a message from the subject (col. 7, line 46).

21. As per claims 14 34 Ramasubramani teaches the PKVC can be verified for authentication by demonstrating knowledge of a private key (col. 11, Lines 42-45).

22. As per claims 15, 35 Ramasubramani teaches the registration authority maintains a certificate database (col. 7, lines 38).

23. As per claim 17, Ramasubramani teaches the credentials server ceases to issue PKVC binding to the first PKVN (col. 12, lines 6-8).

24. As per claim 18, Ramasubramani teaches removing the table entry (col. 12, lines 6-9).

25. As per claim 19, Ramasubramani teaches marking the first unsigned certificate in the database as being invalid (col. 12, lines 6-9 and lines 20-25).

26. As per claim 20, Ramasubramani teaches verifying the request for revocation that includes the previously generated PKRC (col. 12, lines 1-25).

27. Claims 37-47, 49-59 are rejected under 35 U.S.C. 102(e) as being anticipated by Perlman et al, hereinafter Perlman (USP 6,230,266).

28. As per claim 37, Perlman teaches a subject (col. 2, lines 2), a first public key validation agent maintaining a record of the status of the public key (col. 2, lines 1-10), having a high probability of being unique, and a verifier configured to respond to an authentication of the subject and ascertaining the validity of the subject's public key (col. 2, lines 55-60).

29. As per claim 38, Perlman teaches binding the subject's public key to a public key validation number (see Fig 5).

30. As per claim 39, Perlman teaches the PKVN are unique (col. 2, line 3).

31. As per claim 40, Perlman teaches issuing a first certificate indicating the binding (col. 2, lines 1-9).

32. As per claim 41, Perlman teaches issuing a second certificate indicating the validity of the subject's public key (col. 6, lines 60-67).

33. As per claim 42, Perlman teaches the first PKVA is configured to respond to a request for invalidating the subject's public key (col. 2, lines 60-62).

34. As per claim 43, Perlman teaches requiring a first issued certificate in order to issue a second certificate (col. 6, lines 30-35).

35. As per claim 44, Perlman teaches the second certificate is a signed certificate (col . 6, line 34).

36. As per claim 45, Perlman teaches the second certificate is a disposable certificate (col. 6, line 34).

37. As per claims 46 and 47, Perlman teaches an expiration time and date (col. 2, line 5).

38. As per claim 49, Perlman teaches responding to a request for invalidating a subject's public key (col. 2, lines 24-26).

39. As per claim 50, Perlman teaches verifying that the request was submitted by an entity having authorization (col. 4, lines 13-15).

40. As per claim 51, Perlman teaches requiring a revocation code in order to invalidate a subject's public key (col. 6, lines 30-36).

41. As per claim 52, Perlman teaches verifying that the revocation code coincides with previously generated PKRC (col. 6, lines 30-36).

42. As per claim 53, Perlman teaches including altering the maintained record (col. 10, lines 54-59).

43. As per claim 54, Perlman teaches changing the validity status of the public key (col. 10, lines 57).

44. As per claim 55, Perlman teaches removing the maintained record (col. 10, lines 60-62).

45. As per claim 56, Perlman teaches altering accessibility to the maintained record (col. 10, lines 36-40).

46. As per claim 57, Perlman teaches authenticating the subject by verifying one purported identity attribute (col. 11, lines 1-9).

47. As per claim 58, Perlman teaches responding to the assertion of the validity of the subject's public key is based on the maintained record (col. 11, lines 1-9).

48. As per claim 59, Perlman teaches certifying the authenticity of the first PKVN and the identifier (col. 11, lines 1 -5).

49. Claims 9, 1 1-13, 16, 29, 31-33, 36 are rejected under 35 U.S.C. 1O3(a) as being unpatentable over Ramasubramani in view of Andrews (USP 6,324,645).

50. As per claims 9, 16, 29, and 36 Ramasubramani is silent in disclosing maintaining a hash table that contains hashes of valid unsigned PKVC. Andrews teaches maintaining a hash table that contains hashes of valid unsigned PKVC (col. 9, line 59--col. 10, line 7), and would be advantageous to verify that a particular certificate has not been changed. In view of this, it would have been obvious to one of ordinary skill in the art at the time using a hash is a way to maintain the validity of a certificate the invention was made to employ the teaching of Andrews within the system of Ramasubramani because it would insure that a certificate has not been altered. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

51. As per claims 1 1-13 and 31-33, Ramasubramani is silent in disclosing a collision-resistant hash such as SHA-I and MD5. Andrews teaches the use of such collision resistant hash function. Examiner supplies the same rationale for the motivation to combine Andrews and Ramasubramani as recited in the rejection of claims 9 and 29.

52. Claims 48 is rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman in view of Andrews (USP, 4,324,645).

53. As per claim 48, Perlman is silent in disclosing maintaining a hash table that contains hashes of valid unsigned PKVC. Andrews teaches maintaining a hash table that contains hashes of valid unsigned PKVC (col. 9, line 59 col. 10, line 7). Using a hash is a way to maintain the validity of a certificate and would be advantageous to verify that a particular certificate has not been changed. In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Andrews within the system of Perlman because it would insure that a certificate has not been altered. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

Double Patenting

54. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

55. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground

provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

56. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

57. Claims 1-20 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-22 and 42-47 of U.S. Patent No. 6,763,459 to Corella. Although the conflicting claims are not identical, they are not patentably distinct from each other because it would have been obvious to one of ordinary skill in the art at the time the invention was made to remove the verifier disclosed in the patent to Corella, since it has been held that it only requires ordinary skill in the art to eliminate an element and its function. See MPEP § 2144.04; see *In re Karlson*, 311 F.2d 581, 583, 136 USPQ 184, 186 (CCPA 1963); *In re Kuhle*, 526 F.2d 553, 188 USPQ 7 (CCPA 1975).

58. Claims 21-36 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 23-41 and 48-51 of U.S. Patent No. 6,763,459 to Corella. Although the conflicting claims are not identical, they are not patentably distinct from each other because it would have been obvious to one of ordinary skill in the art at the time the invention was made to remove the step of presenting the short-term disposable certificate to the verifier for authentication disclosed in the patent to Corella, since it has been held that it only requires ordinary skill in the art to eliminate an element and its function. See MPEP § 2144.04; see *In re Karlson*, 311 F.2d 581, 583, 136 USPQ 184, 186 (CCPA 1963); *In re Kuhle*, 526 F.2d 553, 188 USPQ 7 (CCPA 1975).

Conclusion

59. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

60. The following patents are cited to further show the state of the art with respect to public key infrastructures, such as:

United States Patent No. 5,850,442 to Muftic, which is cited to show an extended network to permit secure electronic commercial transactions to be achieved.

United States Patent No. 6,009,177 to Sudia, which is cited to show a key escrow feature that uses a method for verifiably splitting user's private encryption keys into components and for sending those components to trusted agents.

United States Patent No. 6,202,150 to Young et al., which is cited to show an escrow system that is overhead free and does not require cryptographic tamper-proof hardware.

United States Patent No. 6,282,295 to Young et al., which is cited to show an escrow system that is overhead free and does not require cryptographic tamper-proof hardware.

United States Patent No. 6,389,136 to Young et al., which is cited to show an escrow system that is overhead free and does not require cryptographic tamper-proof hardware.

United States Patent No. 6,367,013 to Bisbee et al., which is cited to show that public keys are bound to users using digital certificates.

61. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

62. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

63. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100